MINIMAL POLYNOMIAL OF AN EXPONENTIAL AUTOMORPHISM OF $\mathbb{C}^n$

JAKUB ZYGADŁO

ABSTRACT. We show that the minimal polynomial of a polynomial exponential automorphism F of $\mathbb{C}^n$ (i. e. $F = \exp(D)$ where D is a locally nilpotent derivation) is of the form $\mu_F(T) = (T-1)^d$, $d = \min\{m \in \mathbb{N} : D^{\circ m}(X_i) = 0 \text{ for } i = 1, \dots, n\}$.

1. Introduction

Let k be a field of characteristic zero and let A be a k-algebra. Recall that a *k-derivation* of A is a k-linear mapping $D\colon A \to A$ fulfilling the Leibniz rule $D(ab) = D(a)b + aD(b)$. We will write $D^{\circ n}$ for the n-th iterate of D, i. e. $D^{\circ n} = D \circ D^{\circ(n-1)}$ and $D^{\circ 0} = I$ - the identity. If for every $a \in A$ there exists $n = n(a) \in \mathbb{N}$ such that $D^{\circ n}(a) = 0$, derivation D is called *locally nilpotent*.

If D is a locally nilpotent derivation of A, we define the *exponential* of D, denoted $\exp(D)$, by the formula

$$\exp(D)(a) := \sum_{i=0}^{\infty} \frac{1}{i!} D^{\circ i}(a)$$

It is easy to see that $\exp(D)\colon A \to A$ is a k-endomorphism of A. One can also check that if locally nilpotent k-derivations D and E commute (i. e. $D \circ E = E \circ D$), then $\exp(D) \circ \exp(E) = \exp(E) \circ \exp(D) = \exp(D + E)$. Therefore, $\exp(D)$ is an automorphism of A with the inverse $\exp(D)^{-1} = \exp(-D)$. In the paper we prove the following

Theorem. *Let D be a locally nilpotent derivation of $\mathbb{C}[X_1, \dots, X_n]$, $F := (\exp(D)(X_1), \dots, \exp(D)(X_n)\,)\colon \mathbb{C}^n \to \mathbb{C}^n$ and $d := \min\{m \in \mathbb{N} : D^{\circ m}(X_i) = 0 \text{ for } i = 1, \dots, n\}$. Then the minimal polynomial for F equals $\mu_F(T) = (T-1)^d = \sum_{j=0}^{d} (-1)^{d-j} \binom{d}{j} T^j$ (i. e. the mapping $\mu_F(F) = \sum_{j=0}^{d} (-1)^{d-j} \binom{d}{j} F^{\circ j}$ is zero and $p(F) \neq 0$ for any polynomial $p \in \mathbb{C}[T] \setminus \{0\}$ of degree less than d). In particular, we have the following formula for the inverse of F:*

$$F^{-1} = \sum_{j=0}^{d-1} (-1)^j \binom{d}{j+1} F^{\circ j}$$

Date: January 4, 2008.

2000 *Mathematics Subject Classification.* 14R10; 13N15.

2. Preparatory steps

Firstly, we will prove two simple lemmas:

Lemma 1. *Let A be a k-algebra, D - a locally nilpotent k-derivation of A and $a \in A$. If for some $m \geq 1$ and $\alpha_0, \dots, \alpha_{m-1} \in k$ there is an equality*

$$D^{\circ m}(a) = \sum_{i=0}^{m-1} \alpha_i D^{\circ i}(a),$$

then $D^{\circ m}(a) = 0$.

Proof. We will proceed by induction on m. If $m = 1$ we have $D(a) = \alpha_0 a$ and the result is well known (even for $\alpha_0 \in A$, if A has no zero divisors - see for example [2], Prop. 1.3.32), but we will prove it for the sake of completeness. If $D(a) = \alpha_0 a$, then $D^{\circ n}(a) = D^{\circ(n-1)}(\alpha_0 a) = \ldots = D(\alpha_0^{n-1} a) = \alpha_0^n a$ for all $n \in \mathbb{N}$. Because D is locally nilpotent, we must have $D^{\circ n}(a) = 0$ for some n and consequently $\alpha_0 = 0$ or $a = 0$. Now let $m > 1$ and assume that the lemma holds for all $m' < m$. Suppose $D^{\circ m}(a) \neq 0$ and let $M \in \mathbb{N}$ be such that $D^{\circ M}(a) = 0$ and $D^{\circ(M-1)}(a) \neq 0$ (note $M > m$). Set $i_0 := \max\{0 \leq i < m : \alpha_i \neq 0\}$, so we can write $0 = D^{\circ M}(a) = D^{\circ(M-m)}(D^{\circ m}(a)) = D^{\circ(M-m)}\big(\sum_{i=0}^{i_0} \alpha_i D^{\circ i}(a)\big) = \sum_{i=0}^{i_0} \alpha_i D^{\circ i}\big(D^{\circ(M-m)}(a)\big)$. Let $a' := D^{\circ(M-m)}(a)$. Because $\alpha_{i_0} \neq 0$, we have $D^{\circ i_0}(a') = -\sum_{i=0}^{i_0-1} \frac{\alpha_i}{\alpha_{i_0}} D^{\circ i}(a')$ and since $i_0 < m$, we obtain $D^{\circ i_0}(a') = 0$ by the induction hypothesis - this is a contradiction with $D^{\circ i_0}(a') = D^{\circ(M-m+i_0)}(a) \neq 0$. □

Lemma 2. *Let $d > 0$, $i \in \mathbb{N}$ and define*

$$\beta_{d,i} := \sum_{m=0}^{d} (-1)^m \binom{d}{m} m^i$$

We have $\beta_{d,i} = 0$ if and only if $i < d$.

Proof. Equality $\beta_{d,0} = 0$ follows from expansion of $(1-1)^d = 0$ and the case $d = 1$ is obvious. Let $d > 1$, $i > 0$ and proceed by induction on d. We have

$$\beta_{d,i} = \sum_{m=1}^{d} (-1)^m d \binom{d-1}{m-1} m^{i-1} = -d \sum_{m=0}^{d-1} (-1)^m \binom{d-1}{m} (m+1)^{i-1} =$$

$$= -d \sum_{j=0}^{i-1} \binom{i-1}{j} \left(\sum_{m=0}^{d-1} (-1)^m \binom{d-1}{m} m^j \right) = -d \sum_{j=0}^{i-1} \binom{i-1}{j} \beta_{d-1,j}$$

and for $i < d$ we conclude by the induction hypothesis, because all $\beta_{d-1,j} = 0$. To deal with the case $i \geq d$, note that $\beta_{1,i} = -1$ for $i \geq 1$, so $\beta_{2,i} = -d \sum_{j=0}^{i-1} \binom{i-1}{j} \beta_{1,j} > 0$ for $i \geq 2$. Proceeding in this way, we see that $(-1)^d \beta_{d,i} > 0$ for $i \geq d$. □

From now on we will focus our attention on the case $k = \mathbb{C}$ and $A = \mathbb{C}[X_1, \ldots, X_n]$ - the ring of polynomials in n variables. It can be shown that every $\mathbb{C}$-derivation D of A is of the form $D = \sum_{i=1}^n f_i \partial_{x_i}$ for some $f_1, \ldots, f_n \in A$, where $\partial_{x_i} = \frac{\partial}{\partial X_i}$ is the standard differential with respect to X_i.

If $\Phi\colon A \to A$ is a $\mathbb{C}$-endomorphism of A, one can define a polynomial mapping $\Phi_*\colon \mathbb{C}^n \to \mathbb{C}^n$ by

$$\Phi_* = (\Phi(X_1), \ldots, \Phi(X_n))$$

Obviously $I_* = I$ and $(\Phi \circ \Psi)_* = \Psi_* \circ \Phi_*$, so each $\mathbb{C}$-automorphism Φ of A gives rise to a polynomial automorphism Φ_* of the affine space $\mathbb{C}^n$. In particular, if D is a locally nilpotent derivation of A and $\Phi = \exp(D)$, we have an automorphism $F = \exp(D)_* = (\exp(D)(X_1), \ldots, \exp(D)(X_n))$ of $\mathbb{C}^n$, called the *exponential automorphism*.

In [1], the following class of polynomial automorphisms is considered: Let $F = (F_1, \ldots, F_n)$ be a polynomial automorphism of $\mathbb{C}^n$. If there is an univariate polynomial $p(T) \in \mathbb{C}[T] \setminus \{0\}$ such that $p(F) = 0$ (i.e. if $p(T) = a_0 + a_1 T + \ldots + a_m T^m$ this means $a_0 I + a_1 F + \ldots + a_m F^{\circ m} = 0$), then F is called *locally finite*.

It is easy to see that the set $I_F := \{p \in \mathbb{C}[T] : p(F) = 0\}$ forms an ideal in $\mathbb{C}[T]$; its monic generator will be called *minimal polynomial* for F and denoted μ_F. The paper [1] gives many equivalent conditions for F to be locally finite and a formula for a polynomial $p(T)$ such that $p(F) = 0$, provided $F(0) = 0$ (see [1], Th. 1.2). Unfortunately, there is no such result when $F(0) \neq 0$ and it is not easy to find the minimal polynomial μ_F, either. We solve this problem for exponential automorphisms of $\mathbb{C}^n$ in the following section.

3. Main result and its consequences

Theorem (main theorem). *Let D be a locally nilpotent derivation of $\mathbb{C}[X_1, \ldots, X_n]$, $F := \exp(D)_*$ and $d := \min\{m \in \mathbb{N} : D^{\circ m}(X_i) = 0$ for $i = 1, \ldots, n\}$. Then the minimal polynomial for F equals $\mu_F(T) = (T-1)^d$.*

Proof. Note that for $m \in \mathbb{N}$, we have $F^{\circ m} = (\exp(D)^{\circ m})_* = \exp(mD)_*$ (because D commutes with D), so if $F = (F_1, \ldots, F_n)$ then

$$(F^{\circ m})_j = \sum_{i=0}^{d-1} \frac{1}{i!}(mD)^{\circ i}(X_j) = \sum_{i=0}^{d-1} \frac{1}{i!} m^i D^{\circ i}(X_j), \quad j = 1, \ldots, n$$

Since

$$\sum_{m=0}^{d} (-1)^m \binom{d}{m} (F^{\circ m})_j = \sum_{i=0}^{d-1} \frac{1}{i!} \left(\sum_{m=0}^{d} (-1)^m \binom{d}{m} m^i \right) D^{\circ i}(X_j) = \sum_{i=0}^{d-1} \frac{1}{i!} \beta_{d,i} D^{\circ i}(X_j)$$

we conclude by Lemma 2 that $\sum_{m=0}^{d} (-1)^m \binom{d}{m} F^{\circ m} = 0$. This argument shows that the polynomial $(1-T)^d \in I_F = \{p \in \mathbb{C}[T] : p(F) = 0\}$. To prove minimality of its degree, assume for example $d = \min\{m \in \mathbb{N} :$

$D^{\circ m}(X_1) = 0\}$ and suppose that $\mu_F(T) = (T-1)^e$ for some $e < d$. Then $0 = (-1)^e\big(\mu_F(F)\big)_1 = \sum_{m=0}^{e}(-1)^m\binom{e}{m}(F^{\circ m})_1 = \sum_{i=0}^{d-1}\frac{1}{i!}\beta_{e,i}D^{\circ i}(X_1)$ and $\beta_{e,d-1} \neq 0$ by Lemma 2. Therefore $D^{\circ(d-1)}(X_1) = -\sum_{i=0}^{d-2}\frac{1}{i!}\frac{\beta_{e,i}}{\beta_{e,d-1}}D^{\circ i}(X_1)$ and due to Lemma 1 we get $D^{\circ(d-1)}(X_1) = 0$, despite the definition of d - a contradiction. $\square$

Corollary. *Since $\mu_F(F) = 0$, we have $I = \left(\sum_{m=1}^{d}(-1)^{m-1}\binom{d}{m}F^{\circ(m-1)}\right)\circ F$ and therefore the inverse of F is given by*

$$F^{-1} = \sum_{m=0}^{d-1}(-1)^m\binom{d}{m+1}F^{\circ m}$$

Remark 1. The famous Nagata automorphism of $\mathbb{C}^3$ (see [3]) defined by $N = (X - 2Y\sigma - Z\sigma^2, Y + Z\sigma, Z)$ where $\sigma = XZ + Y^2$ can be seen as an exponential of a locally nilpotent derivation $D = -2Y\sigma\partial_x + Z\sigma\partial_y$ of $\mathbb{C}[X,Y,Z]$. It is easy to check that $D(\sigma) = 0$ and $D^{\circ 3}(X) = D^{\circ 3}(Y) = D^{\circ 3}(Z) = 0$, so the main theorem gives $\mu_N(T) = (T-1)^3$, whereas by ([1], Th. 1.2) we only get that $p(T) = (T-1)^{55} \in I_N$.

Remark 2. Let $d \geq 2$ and $D = Y^{d-2}\partial_x + \partial_y$. Obviously D is a locally nilpotent derivation of $\mathbb{C}[X,Y]$ and $D^{\circ d}(X) = D^{\circ d}(Y) = 0$ (d is minimal). If we let $F = \exp(D)_*$, then $\mu_F(T) = (T-1)^d$ by the main theorem. Since clearly $\deg F = d-2$, this shows that the estimate $\deg \mu_F \leq \deg F + 1$ ([1], Th. 4.2) need not hold if $F(0) \neq 0$.

Remark 3. Recall that if $P = (P_1, \ldots, P_n)\colon \mathbb{C}^n \to \mathbb{C}^n$ is a polynomial mapping, then P^* given by $P^*(X_i) := P_i \in \mathbb{C}[X_1, \ldots, X_n]$ defines a $\mathbb{C}$-endomorphism of $\mathbb{C}[X_1, \ldots, X_n]$. Let $F = (X + g(Y,Z), Y + h(Z), Z)$ be an upper triangular automorphism of $\mathbb{C}^3$ ($g \in \mathbb{C}[Y,Z]$, $h \in \mathbb{C}[Z]$). If $g = 0$ or $h = 0$, then F is easily seen to be an exponential of a locally nilpotent derivation of $\mathbb{C}[X,Y,Z]$. So let us suppose that $g \neq 0$ and $h \neq 0$. We will show that the minimal polynomial for F equals $\mu_F(T) = (T-1)^d$, where $d := 2 + \deg_Y g$ and therefore in this case we also have $F = \exp(D)_*$ (see [1], Th. 2.3) for the locally nilpotent derivation D given by the following formula: $D = \sum_{m=1}^{+\infty}\frac{(-1)^{m+1}}{m}(F^* - I^*)^{\circ m}$ (cf. [2], Ch. 2). Obviously $D(Z) = 0$, $D(Y) = h(Z)$ and one can use above formula to evaluate $D(X)$ - note that if we can show that the minimal polynomial has degree d, then only first $d-1$ summands are nonzero. Write $g(Y,Z) = \sum_{i=0}^{d-2} Y^i g_i(Z)$. Iterating F, we get

$$F^{\circ m} = (X + \sum_{j=0}^{m-1}\sum_{i=0}^{d-2}\big(Y + jh(Z)\big)^i g_i(Z), Y + mh(Z), Z) =$$

$$= (X + \sum_{i=0}^{d-2} g_i(Z)\sum_{k=0}^{i}\binom{i}{k}Y^{i-k}h(Z)^k\sum_{j=0}^{m-1}j^k, Y + mh(Z), Z)$$

Let $s_k(m) := \sum_{j=0}^{m-1} j^k$ and note that s_k is a polynomial in m of degree $k+1 \leq d-1 < d$. Therefore, Lemma 2 gives $\sum_{m=0}^{d}(-1)^m \binom{d}{m} s_k(m) = 0$ for all $k \leq d-2$ and we can argue as in the proof of the main theorem (since $g_{d-2}(Z)h(Z)^{d-2}s_{d-2}(m)$ is the only term involving m^{d-1}, we must have $D^{\circ(d-1)}(X) \neq 0$). Consequently $\mu_F(T) = (T-1)^d$ and $F = \exp(D)_*$, where

$$D = \left(\sum_{m=1}^{d-1} \sum_{i=1}^{m} \frac{(-1)^{i+1}}{m} \binom{m}{i} \big((F^{\circ i})_1 - X \big) \right) \partial_x + h(Z)\partial_y$$

and $d = 2 + \deg_Y g$. Note that d is minimal and easily found in this case (there are obstacles to calculations of the minimal degree, cf. [1], Th. 1.2).

References

[1] J.-P. Furter, S. Maubach, *Locally Finite Polynomial Endomorphisms*, J. Pure and Applied Algebra, **211**(2) (2007), pp. 445-458.

[2] A. van den Essen, *Polynomial Automorphisms and the Jacobian Conjecture*, Progress in Math., vol. 190, Birkhäuser Verlag, Basel, Boston, Berlin, 2000.

[3] M. Nagata, *On the automorphism group of $k[X,Y]$*, in: Kyoto Univ. Lectures in Math. vol. 5, Kyoto University, Kinokuniya, Tokio, 1972.

Institute of Mathematics, Jagiellonian University, Reymonta 4, 30-059 Kraków, Poland.

E-mail address: jakub.zygadlo@im.uj.edu.pl